



AML/CTF Compliance Policy

IN-AML-007-03

Approval date: 05 Dec 2025

Effective date: 08 Dec 2025

Signed by and on behalf of **Vavada B.V.**:

Name: **Boy Hendriks** on behalf of Ecorpp Management N.V.

Title: **Director**

Table of Contents

1. Policy Statement.....	3
2. Purpose.....	3
3. Audience.....	4
4. Definitions.....	4
5. Business Risk Assessment.....	6
6. Customer Risk Assessment.....	6
7. Customer Acceptance Policy.....	6
8. Customer Due Diligence.....	7
9. Purpose and Intended Nature of the Business Relationship.....	8
10. Timing of CDD Measures.....	8
11. Ongoing Monitoring.....	9
12. Reliance on Third Parties to Perform CDD.....	9
14. Suspicious Activity Reporting.....	10
15. Prohibition on tipping-off.....	10
16. Anti-Money Laundering Compliance Programme.....	10
17. Employee screening.....	11
18. Compliance and Consequences of Non-Compliance.....	12
19. Related Information.....	12
20. Contact Information.....	12
21. Policy History.....	13
22. Policy URL.....	13
Appendix A: VAVADA B.V. Prohibited Jurisdictions.....	14

1. Policy Statement

- 1.1. This Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy (“the Policy”) sets out the principles, standards and internal controls adopted by VAVADA B.V. (“the Company”) to prevent and detect money laundering, terrorism financing and proliferation financing in connection with its gaming activities.
- 1.2. The Policy applies to all Company directors, officers, employees, and any third parties acting on behalf of the Company in Curaçao and in any other jurisdictions where the Company operates.
- 1.3. The Curaçao Gaming Control Board, acting as the Curaçao Gaming Authority (CGA), is the supervisory authority for AML/CFT/CFP compliance in the Curaçao gaming sector. This Policy, and the Company's AML/CTF programme, are designed to comply with and implement the CGA's AML/CFT/CFP Regulations applicable to online gaming operators.
- 1.4. This Policy is designed to ensure compliance with the applicable Curaçao AML/CTF framework, including, but not limited to:
 - i. the National Ordinance on Identification when rendering Services (NOIS);
 - ii. the National Ordinance on the Reporting of Unusual Transactions (NORUT);
 - iii. the Sanctions National Ordinance (N.G. 2014 no. 55);
 - iv. the Kingdom Sanction Act (N.G. 2016 no. 54); and
 - v. the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction issued by the Curaçao Gaming Control Board (CGA).
- 1.5. In case of any conflict between this Policy and applicable law, the stricter requirement shall prevail.
- 1.6. This Policy and the underlying AML/CTF/CFP programme are approved by the Board of Directors (or, where applicable, senior management) and are reviewed at least annually, and earlier where there are material changes to the Company's business, risk profile or applicable laws and regulations.
- 1.7. The Company shall make this Policy, the detailed AML/CTF/CFP procedures, and the records of its Business Risk Assessment, Customer Risk Assessment and unusual transaction reports readily available to the Curaçao Gaming Authority upon request, in line with the CGA Regulations.

2. Purpose

The purpose of this Policy is to:

- 2.1. ensure that the Company identifies, assesses and mitigates the risks of money laundering, terrorism financing and proliferation financing related to its gaming activities;
- 2.2. set out clear and risk-based standards for Business Risk Assessment and Customer Risk Assessment in line with GCB Regulations and FIU Curaçao guidance;
- 2.3. define minimum Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) requirements, including ongoing monitoring of customers and transactions;
- 2.4. describe the internal controls, governance arrangements and responsibilities (including the MLRO function) that support the Company's AML/CTF compliance programme;

- 2.5. ensure that unusual transactions are identified and reported to FIU Curaçao in accordance with the applicable law.

3. Audience

This Policy applies to:

- 3.1. all directors and members of senior management of the Company;
- 3.2. all employees of the Company, irrespective of their position, department or location;
- 3.3. any agents, payment processors, affiliates, and other third parties who provide services to or act on behalf of the Company under contractual arrangements, to the extent relevant to their role in the provision of gaming services.
- 3.4. the extent relevant, to all subcontractors, suppliers and outsourced service providers involved in the provision of gaming services, compliance support, identity verification, payment processing, technical support or any other functions that may be relevant to the Company's AML/CTF/CFP obligations. The Company shall ensure through appropriate contractual arrangements that such parties are required to comply with AML/CTF standards that are consistent with this Policy and the applicable Curaçao AML/CTF framework.

4. Definitions

For the purposes of this Policy, the following terms shall have the meanings set out below:

- 4.1. **AML (Anti-Money Laundering):** Measures and policies aimed at preventing the laundering of money obtained illegally and financing terrorism.
- 4.2. **Business relationship:** a relationship between the Company and a customer which, at the time when contact is established, is expected to have an element of duration.
- 4.3. **FT (Financing Terrorism):** Financial support for acts of terrorism or terrorist organizations.
- 4.4. **CFP or FP:** means combating the financing of proliferation of weapons of mass destruction.
- 4.5. **Client:** An individual (natural person) using the Company's services
- 4.6. **Curaçao Gaming Authority or CGA:** the Curaçao Gaming Control Board acting as the supervisory authority for AML/CFT/CFP compliance in the Curaçao gaming sector.
- 4.7. **GCB Regulations:** the AML/CFT/CFP regulations, guidance and other instruments issued by the Curaçao Gaming Authority from time to time.
- 4.8. **Beneficial Owner:** By using the website, the Client confirms that they are the beneficial owner of the funds used for gaming purposes. A beneficial owner is defined as the individual (natural person) who ultimately owns or controls the funds or assets used in transactions or activities on the platform, acting solely on their own behalf without the involvement of any third party or intermediary.
- 4.9. **High-risk jurisdiction:** a country or territory identified by the Company as presenting a higher risk of money laundering, terrorism financing or proliferation financing, taking into account, inter alia, the lists and public statements issued by the FATF and the Curaçao authorities.

- 4.10. **Prohibited jurisdiction:** a country or territory from which the Company does not accept customers and to which it does not intentionally provide its gaming services, as set out in Appendix A and any updates thereto
- 4.11. **KYC (Know Your Client):** A policy for verifying and identifying Clients to assess their risk levels.
- 4.12. **DD (Due Diligence):** A process of investigation or auditing to ensure compliance with laws, regulations, and ethical standards.
- 4.13. **Customer Due Diligence** or **CDD** means the set of measures applied to identify and verify the customer and, where applicable, the beneficial owner, to understand the purpose and intended nature of the business relationship, and to perform ongoing monitoring, in accordance with applicable AML/CFT/CFR requirements.
- 4.14. **Enhanced Due Diligence** or **EDD:** additional CDD measures applied to higher-risk customers, products, services or transactions, as determined on a risk-based basis, including but not limited to customers from high-risk jurisdictions and PEPs.
- 4.15. **MLRO (Money Laundering Reporting Officer):** A designated individual responsible for overseeing and ensuring the implementation of AML policies and reporting suspicious activities.
- 4.16. **FATF (Financial Action Task Force):** An international organization that sets standards and promotes effective implementation of AML and FT measures.
- 4.17. **OFAC (Office of Foreign Assets Control):** A U.S. government agency that administers sanctions against designated individuals, groups, and entities.
- 4.18. **PEP (Politically Exposed Person):** An individual who holds or has held a high-ranking public office, along with their close associates and family members.
- 4.19. **STR/SAR (Suspicious Transaction Report/Suspicious Activity Report):** Reports filed to regulatory authorities when suspicious or unusual activities are detected.
- 4.20. **FIU (Financial Intelligence Unit):** A government agency responsible for collecting and analyzing information to combat financial crimes like money laundering and terrorism financing.
- 4.21. **Risk-Based Approach:** A method of assessing and managing risks based on their likelihood and impact, especially in Client relationships.
- 4.22. **Sanctioned List:** A list of individuals, entities, or countries subject to trade restrictions or financial penalties.
- 4.23. **Tipping-off:** any act of disclosing to a customer or a third party that an internal or external report of an unusual or suspicious transaction has been, will be or may be made, or that the customer is being, or may be, subject to investigation in connection with ML/TF/FP concerns.
- 4.24. **Prohibited Jurisdictions:** Countries or regions where the Company is not permitted to conduct transactions due to legal or regulatory restrictions.
- 4.25. **Unusual transaction:** means a transaction that is considered unusual on the basis of indicators adopted under Article 10 of the NORUT and relevant implementing decrees and guidance.
- 4.26. **Suspicious transaction:** means a transaction which, based on the facts, context and the Company's knowledge of the customer, gives rise to a reasonable ground to suspect that funds are the proceeds of crime or are related to the financing of terrorism or proliferation.
- 4.27. **Money Laundering Reporting Officer** or **MLRO** means the person appointed by the Company who is responsible for receiving and assessing internal reports of unusual or suspicious transactions,

making external reports to FIU Curaçao and overseeing the implementation of the AML/CTF/CFP programme.

5. Business Risk Assessment

- 5.1. The Company conducts and maintains a documented Risk-Based Approach (“RBA”) to identify and assess the money laundering, terrorism financing and proliferation financing risks to which its gaming activities are exposed.
- 5.2. The RBA considers:
 - i. the types of customers and customer segments;
 - ii. the products and services offered (including payment methods and delivery channels);
 - iii. geographical risk factors, including countries and regions where customers are located or where transactions originate;
 - iv. relevant findings from the National Risk Assessment(s) of the jurisdictions where the Company operates.
- 5.3. The RBA is reviewed at least annually and whenever there are material changes to the Company’s business model, products, markets or regulatory framework. The RBA is approved by the Board of Directors and made available to the Curaçao Gaming Control Board upon request.

6. Customer Risk Assessment

- 6.1. For each customer, the Company performs a Customer Risk Assessment (“CRA”) at the time of establishing a business relationship or carrying out an occasional transaction that reaches the applicable thresholds.
- 6.2. The CRA takes into account at least:
 - i. the customer’s identity, profile and behaviour (including occupation, source of funds and source of wealth where applicable);
 - ii. the customer’s country of residence and/or nationality;
 - iii. the products, services and payment methods used by the customer;
 - iv. the interface and delivery channels used by the customer (e.g. online, mobile).
- 6.3. Based on the CRA, customers are classified as low, medium or high risk. The CRA determines the applicable level of Customer Due Diligence (CDD), including ongoing monitoring measures.
- 6.4. Customer risk ratings are reviewed periodically and whenever there is a trigger event (e.g. change in behaviour, large transaction, adverse media, sanctions/PEP hit).

7. Customer Acceptance Policy

- 7.1. The Company applies a documented Customer Acceptance Policy (“CAP”) which sets out:
 - i. the types of customers that the Company is prepared to onboard;

- ii. customer categories and risk indicators that may result in a higher-than-average risk (e.g. PEPs, customers from high-risk jurisdictions, adverse media);
 - iii. the level of CDD/EDD and ongoing monitoring applicable to each risk category;
 - iv. circumstances under which the Company will refuse to enter into, or will terminate, a business relationship (including when CDD cannot be completed, when the customer is a sanctioned person, or when there are reasonable grounds to suspect ML/TF).
- 7.2. When drawing up and applying its CAP, the Company complies with its obligations regarding Politically Exposed Persons (PEPs) and sanctions screening in accordance with the applicable Curaçao AML/CTF regime.

8. Customer Due Diligence

- 8.1. The Company performs Customer Due Diligence (“CDD”) measures before or during the establishment of a business relationship and prior to carrying out an occasional transaction that meets or exceeds the applicable legal thresholds.
- 8.2. As a minimum, CDD includes:
- i. identifying the customer and verifying their identity on the basis of reliable and independent documents, data or information (e.g. passport, ID card, residence permit);
 - ii. identifying and, where applicable, verifying the beneficial owner;
 - iii. understanding the purpose and intended nature of the business relationship;
 - iv. screening the customer against relevant sanctions lists and PEP lists.
- 8.3. For any single transaction or a series of linked transactions equal to or exceeding 4000 NAf (or equivalent), the Company performs CDD in line with applicable Curaçao regulations.
- 8.4. Enhanced Due Diligence (“EDD”) is performed for:
- i. transactions equal to or exceeding 5000 NAf (or equivalent), where required by the applicable Indicators Regulation;
 - ii. high-risk customers (including PEPs and customers from high-risk jurisdictions);
 - iii. any situation where there is an increased risk of ML/TF.
- 8.5. Where required by law, or upon instruction of FIU Curaçao or another competent authority, the Company will freeze or block funds or accounts related to a customer and refrain from executing a transaction until further instructions have been received.
- 8.6. Beneficial Owner Identification and Verification
- 8.7. For legal persons and legal arrangements, the Company shall identify and verify the identity of the beneficial owner(s) (“BOs”) and understand the customer's ownership and control structure.
- 8.8. As a minimum, the Company shall:
- i. obtain information on the ownership and control structure, including all intermediate layers up to the natural persons who ultimately own or control the customer;

- ii. identify all natural persons who directly or indirectly own or control 25% or more of the shares or voting rights of the customer, or who otherwise exercise ultimate effective control over the customer; and
 - iii. take reasonable measures to verify the identity of such beneficial owners using reliable and independent documents, data or information.
- 8.9. Where no natural person can be identified on the basis of ownership or control, the Company shall identify the natural person who holds the position of senior managing official as the beneficial owner for CDD purposes.
- 8.10. Where required by law, or upon instruction of FIU Curaçao, the Curaçao Gaming Authority or any other competent authority, or where the MLRO determines that there are reasonable grounds to suspect money laundering, terrorism financing or proliferation financing, the Company shall immediately freeze or block the relevant customer funds or accounts and refrain from executing any related transactions until further written instruction has been received.
- 8.11. The MLRO shall ensure that FIU Curaçao and, where required, the Curaçao Gaming Authority are notified of such action as soon as practicable and, in any event, within 24 hours of the freezing action, in line with the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance and the applicable CGA AML/CTF/CFP Regulations.

9. Purpose and Intended Nature of the Business Relationship

- 9.1. For each business relationship, the Company shall obtain information on the purpose and intended nature of the relationship, proportionate to the customer's risk profile.
- 9.2. At a minimum, the Company shall:
- i. understand why the customer is seeking to use the Company's gaming services and how the account is expected to be used; and
 - ii. collect sufficient information, and where necessary documentation, to establish the customer's source of wealth and expected level and pattern of activity.
- 9.3. The extent of information collected shall be consistent with the ML/TF/FP risk identified in the Customer Risk Assessment. Where the risk is not high, a customer declaration (e.g. nature of employment/business and usual annual income) may be sufficient. For higher-risk customers, more detailed information and corroborating documentation shall be obtained.

10. Timing of CDD Measures

- 10.1. The Company applies the timing rules for Customer Due Diligence (CDD) measures in line with the AML/CTF/CFP Regulations issued by the Curaçao Gaming Authority and the NOIS/NORUT framework.
- 10.2. Upon opening an account, the Company collects, as a minimum, the following personal details of the customer: full name, permanent residential address and date of birth, and performs sanctions screening. These measures are applied simultaneously with the establishment of the business relationship, at least in low-risk situations.
- 10.3. The Company calculates on a daily basis whether a customer's cumulative financial transactions (including deposits, withdrawals and peer-to-peer transfers) reach or exceed the 4000 NAF threshold (or equivalent in other currency).

- 10.4. All required CDD measures – including full identification and verification of the customer, Customer Risk Assessment and PEP and sanctions screening – must be completed by the time the 4000 NAF threshold is reached.
- 10.5. While CDD measures are being carried out, customers may be allowed to continue using their gaming account. However, once the 4000 NAF threshold has been reached, the customer may not deposit funds into the account or withdraw funds from the account until CDD has been completed.
- 10.6. If the requested CDD information and documentation is not received within 30 days from the date on which the 4000 NAF threshold was first reached, the Company shall terminate the business relationship with the customer and report the transaction to FIU Curaçao in accordance with the applicable legislation.

11. Ongoing Monitoring

- 11.1. The Company conducts ongoing monitoring of its business relationships and transactions to ensure that they remain consistent with the customer's known profile, risk rating and expected behaviour.
- 11.2. Ongoing monitoring includes:
 - i. periodic review and update of customer identification data and risk profiles;
 - ii. monitoring of transactions to identify patterns, volumes and behaviours that are inconsistent with the customer's profile or known source of funds;
 - iii. review and, where necessary, escalation of alerts generated by automated monitoring systems or manual review.
- 11.3. Where ongoing monitoring identifies unusual activity or red flags, the case is escalated to the MLRO for further investigation and, where appropriate, reporting to FIU Curaçao.

12. Reliance on Third Parties to Perform CDD

- 12.1. The Company may rely on third-party service providers to perform certain CDD measures (e.g. electronic identity verification, document validation, biometric checks), provided that:
 - i. such third parties are subject to AML/CTF requirements that are consistent with the Curaçao AML/CTF framework; and
 - ii. the Company remains ultimately responsible for compliance with all applicable CDD obligations.
 - 12.2. The Company maintains written agreements with third-party KYC providers, performs periodic reviews of their performance and retains immediate access to all underlying customer identification data and documents obtained through such third parties.
13. Reporting of Unusual Transactions
- 13.1. The Company identifies and reports unusual transactions in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT) and related regulations and guidance issued by FIU Curaçao and the GCB.
 - 13.2. The MLRO is responsible for:

- i. assessing internal reports and determining whether a transaction is unusual under the applicable indicators;
 - ii. filing an Unusual Transaction Report with FIU Curaçao without undue delay and within the legal deadlines;
 - iii. maintaining records of all internal and external reports, including the rationale for reporting or not reporting.
- 13.3. All unusual individual transactions or series of transactions, as defined in the applicable Indicators Regulation, must be reported internally and, where applicable, externally to FIU Curaçao.
- 13.4. Employees are prohibited from tipping off customers or third parties about any internal or external reporting related to unusual or suspicious transactions.

14. Suspicious Activity Reporting

- 14.1. Under the NORUT framework, the Company's legal obligation is to identify and report "unusual transactions" to FIU Curaçao on the basis of objective and subjective indicators.
- 14.2. Internally, the Company also uses the term "suspicious transaction" for cases where staff or the MLRO consider that there are reasonable grounds to suspect ML/TF/FP. Suspicious transactions will always be treated as unusual transactions for NORUT reporting purposes, but an unusual transaction does not always require that ML/TF/FP suspicion exists.
- 14.3. The MLRO shall ensure that:
 - i. all transactions that meet the applicable unusual transaction indicators are identified and, where required, reported to FIU Curaçao without undue delay; and
 - ii. cases giving rise to ML/TF/FP suspicion are documented and assessed, and where appropriate, reported as unusual transactions under NORUT.

15. Prohibition on tipping-off

- 15.1. Directors, officers, employees and any third parties acting on behalf of the Company are strictly prohibited from disclosing to a customer or to any other third party that:
 - i. an internal report of an unusual or suspicious transaction has been made;
 - ii. an Unusual Transaction Report has been, will be or may be filed with FIU Curaçao; or
 - iii. the customer is being, or may be, subject to CDD/EDD or investigation in connection with ML/TF/FP concerns.
- 15.2. Any breach of the tipping-off prohibition may result in disciplinary action and, where applicable, may be reported to the competent authorities.

16. Anti-Money Laundering Compliance Programme

- 16.1. The Company maintains a risk-based AML/CTF compliance programme which includes, at a minimum:

- i. clear allocation of responsibilities, including the appointment of a Money Laundering Reporting Officer (MLRO) with sufficient authority, independence and resources;
 - ii. documented policies, procedures and controls covering CDD/EDD, ongoing monitoring, sanctions screening, record-keeping and reporting of unusual transactions;
 - iii. a documented Risk Based Approach framework;
 - iv. initial and ongoing AML/CTF training for all relevant employees, tailored to their role and responsibilities;
 - v. periodic testing and review of the effectiveness of the AML/CTF controls and remediation of any identified weaknesses.
- 16.2. The AML/CTF programme shall be subject to an independent audit at least annually in order to test its effectiveness and compliance with applicable laws and regulations.
- 16.3. The independent audit may be performed by:
 - i. an appropriately qualified internal audit function that is independent from the AML compliance function and day-to-day gaming operations; or
 - ii. an appropriately qualified external independent party.
- 16.4. The independent audit shall, at a minimum, include:
 - i. a review of the AML/CTF/CFP policies, procedures and manuals;
 - ii. testing of a sample of customer files and transactions, including unusual transactions and frozen accounts;
 - iii. assessment of the effectiveness of CDD/EDD, ongoing monitoring, sanctions screening and reporting procedures;
 - iv. evaluation of the adequacy of staff training and record-keeping; and
 - v. verification of compliance with applicable Curaçao laws, NORUT/NOIS obligations and CGA Regulations.
- 16.5. The scope and results of each audit shall be documented, and any deficiencies or recommendations shall be reported to senior management and, where appropriate, the Board for timely remedial action.

17. Employee screening

- 17.1. The Company maintains an employee screening programme proportionate to its size and risk profile, covering pre-employment screening and ongoing screening for relevant staff.
- 17.2. At a minimum, the Company shall:
 - i. perform pre-employment screening for employees in AML-relevant roles (including senior management, MLRO, compliance, payments, VIP and customer support), which may include verification of identity, employment history, qualifications and checks for conflicts of interest, integrity and criminal background, in accordance with applicable labour and data protection laws; and

- ii. conduct ongoing screening of such staff, on a risk-based basis, including periodic checks against relevant sanctions and PEP lists and review of any new information that may affect their fitness and propriety.

17.3. The scope and frequency of employee screening shall be documented and approved by senior management.

18. Compliance and Consequences of Non-Compliance

18.1. Compliance with this Policy is mandatory for all persons within its scope (see section Audience).

18.2. Any breach of this Policy, whether intentional or due to gross negligence, may result in:

- i. internal disciplinary action, up to and including termination of employment or contract, in line with the Company's HR policies and local labour laws; and
- ii. where applicable, reporting to FIU Curaçao, the GCB or other competent authorities, as required by law.

18.3. Failure by the Company to comply with applicable AML/CTF laws and regulations may result in administrative measures or sanctions imposed by the GCB or other competent authorities, as well as criminal sanctions where provided for by law.

19. Related Information

This Policy should be read in conjunction with the following internal and external documents (as amended from time to time):

19.1. the Company's Terms and Conditions and Responsible Gambling Policy;

19.2. applicable Curaçao AML/CTF legislation, including:

- i. National Ordinance on Identification when rendering Services (NOIS);
- ii. National Ordinance on the Reporting of Unusual Transactions (NORUT);
- iii. Sanctions National Ordinance (N.G. 2014, no. 55);
- iv. Regulations for the combating of Money Laundering and the Financing of Terrorism and Proliferation issued by the GCB;
- v. indicators and guidance issued by FIU Curaçao.

20. Contact Information

Questions about this Policy or its implementation should be addressed to the Company's Money Laundering Reporting Officer (MLRO):

Mr. Egor Kolotilov

Title: Money Laundering Reporting Officer

Email: mlro@vavada.com

21. Policy History

Version	Effective Date	Summary of Changes
n/a	13 Jul 2024	Initial AML Compliance Policy issued
POL-AML-007-02	24 Feb 2025	Update to reflect regulatory changes
IN-AML-007-03	08 Dec 2025	Alignment with regulatory AML/CTF Policy Template and Regulations

22. Policy URL

- 22.1. This Policy is maintained in the Company's internal document management system and is available to all employees and relevant third parties upon request. It is also made available to the Curaçao Gaming Control Board and other competent authorities upon request.
- 22.2. The Policy is not published on the public Company website.

Appendix A: VAVADA B.V. Prohibited Jurisdictions

COUNTRIES:		
Abkhazia	Guyana	Tristan da Cunha
Afghanistan	Haiti	Saint Kitts and Nevis
American Samoa	Hong Kong	Saint Vincent and the Grenadines
Anguilla	Iran	Saint-Martin
Antigua and Barbuda	Iraq	Saint-Pierre and Miquelon
Aruba	Isle of Man	Sao Tome and Principe
AUSTRALIA	Jersey	Serbia
Azad Kashmir	Kosovo	Seychelles
Barbados	Libya	Sierra Leone
Bermuda	Lugansk People's Republic	Singapore
Bonaire	Macau	Sint Eustatius
British Virgin Islands	Malawi	Sint Maarten
Canada	Marshall Islands	Slovakia
Cape Verde	Martinique	Solomon Islands
Cayman Islands	Mayotte	Somalia
Chad	Montenegro	South Ossetia
Christmas Island	Montserrat	South Sudan
Cocos (Keeling) Islands	Myanmar	State of Palestine
Comoro Islands	Netherlands	Sudan
Cook Islands	New Caledonia	Sweden
Cuba	Niue	Syria
Curacao	Norfolk	Turkish Republic of Northern Cyprus
Donetsk People's Republic	North Korea	Tokelau
East Timor	Northern Mariana Islands	Transnistria
Eritrea	Palau	Trinidad and Tobago
Falkland Islands	Pitcairn	Turks and Caicos Islands
Faroe Islands	Portugal	Tuvalu
Federated States of Micronesia	Republic of Artsakh	Uganda
France	Republic of the Congo	United Kingdom
French Guiana	Réunion	United States of America (USA)
Germany	Crimea	Vatican City
Gibraltar	Rwanda	Virgin Islands of the United States
Grenada	Saba	Wallis and Futuna
Guadeloupe	Sahrawi Arab Democratic Republic	Yemen
Guam	Saint Barthelemy	Belgium
Guernsey	Saint Helena, Ascension and	Spain
South Africa	Nigeria	Cambodia
China	Saudi Arabia	Switzerland
Lithuania		

The Company does not accept customers who are resident, located or accessing the Website from:

1. the countries and territories listed below; and
2. any jurisdiction that is, from time to time:
 - a. subject to a comprehensive country-wide sanctions regime under United Nations, European Union, Kingdom Sanction Act or Sanctions National Ordinance; or
 - b. included in the FATF list of High-Risk Jurisdictions subject to a Call for Action.

This list forms part of the Company's Business Risk Assessment and Customer Acceptance Policy and may be updated on a risk-based basis.